

Scenario: Turning On BitLocker Drive Encryption on a Fixed or Removable Data Drive (Windows 7)

Applies To: Windows 7

This scenario provides the procedure for turning on BitLocker Drive Encryption protection on a fixed or removable data drive on a computer.

Caution

When encrypting a removable drive, do not suddenly remove the drive. If you need to remove a drive before encryption is complete, pause the encryption process and then use either the **Safely Remove Hardware** icon from the notification area or the **Eject** command from Windows Explorer to remove the drive. Removing the drive during the encryption process without pausing and intentionally removing the device can cause the data on the drive to be corrupted.

Why should you encrypt your data?

Data encryption is a method of disguising your data. Therefore, even if someone did get ahold of your flash drive that had video data on it, they wouldn't be able to see it without having a password to decrypt it. One way to encrypt your data is with *TrueCrypt*. *TrueCrypt* is a "free open-source disk encryption software". The following steps will walk you through how to encrypt your flash drive using *TrueCrypt*.

What You'll Need:

- Computer with Internet Access
- Clean Flash Drive (8-16GB+)

BEFORE YOU START: Make sure that no data is on the flash drive that you plan on encrypting since it could potentially get erased in the process of formatting or encrypting!

Before you start

To complete the procedure in this scenario:

- You must be able to provide administrative credentials to turn on BitLocker for fixed data drives. Standard user accounts can turn on BitLocker To Go on removable data drives.

- You must be able to configure a printer if you want to print the recovery key.
- Your computer must meet BitLocker requirements. For more information, see "Requirements for BitLocker Drive Encryption" in [BitLocker Drive Encryption Step-by-Step Guide for Windows 7](#).

To turn on BitLocker Drive Encryption on a fixed or removable data drive

1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.
2. Click **Turn On BitLocker** for the fixed or removable data drive that you want to encrypt.

Note:

If you have configured the Group Policy settings in your organization to back up BitLocker recovery information to Active Directory Domain Services (AD DS), the computer must be able to connect to the domain to complete this process.

3. The BitLocker setup wizard will ask you how you want to unlock this drive. Fixed data drives can be configured to automatically unlock when the operating system drive is encrypted, to unlock after a password is supplied, or to unlock after a smart card is inserted. Removable data drives can be configured to unlock after a password is supplied or to unlock after a smart card is inserted. If you want the removable data drive to automatically unlock, you can specify that option after encryption has occurred by clicking **Manage BitLocker** from the **BitLocker Drive Encryption** Control Panel item or by selecting the **Automatically unlock on this computer from now on** check box when you unlock the drive.
4. Before BitLocker encrypts the drive, the BitLocker setup wizard prompts you to choose how to store the recovery key. You can choose from the following options:
 - **Save the recovery key to a USB flash drive.** Saves the recovery key to a USB flash drive. This option cannot be used with removable drives.
 - **Save the recovery key to a file.** Saves the recovery key to a network drive or other location.
 - **Print the recovery key.** Prints the recovery key.

Use one or more of these options to preserve the recovery key. For each option that you select, follow the wizard steps to set the location for saving or printing the recovery key. When you have finished saving the recovery key, click **Next**.

Important

The recovery key is required when a BitLocker-protected fixed data drive configured for automatic unlocking is moved to another computer, or the password or smart card associated with unlocking the fixed or removable drive is not available, such as when a password is forgotten or a smart card is lost. You will need your recovery key to unlock the encrypted data on the drive if BitLocker enters a locked state. This recovery key is unique to this particular drive. You cannot use it to recover encrypted data from any other BitLocker-protected drive.

For maximum security, you should store recovery keys apart from the drives they are associated with.

5. The BitLocker setup wizard asks if you are ready to encrypt the drive. Click **Start Encrypting**.
6. The **Encrypting** status bar is displayed. You can monitor the ongoing completion status of the drive encryption by moving the mouse pointer over the **BitLocker Drive Encryption** icon in the notification area, at the far right of the taskbar.

By completing this procedure, you have encrypted a fixed or removable data drive, associated a key protector with an unlock method for the drive, and created a recovery key that is unique to this drive

Additional support

If you have need of further help then please contact the UWO Help Desk at 920-424-3020 or visit them at Dempsey Room 207.